## REMARKS/ARGUMENTS

Claims 1-8 are pending in the application. Claims 1-8 stand rejected under 35 U.S.C. 103(a).

### *Amendments*

The third paragraph on page 4 of the disclosure is amended to correct minor editorial issues in translation of the specification. See, e.g., p. 6, lines 1 –17.

Amended independent claim 1 proposes a procedure for the increased security of authentication processes in digital mobile radio systems that involves storing several different secret SIM-specific keys (KI) in a mobile radio network and in a subscriber identification module (SIM), pre-configuring and storing a RAND/SRES/KC authentication triplet for each one of the several secret keys (K1) stored in the mobile radio network, and selecting and sending a random value RAND of one of the pre-configured authentication triplets to the subscriber identification module (SIM) by the mobile radio network. Amended claim 1 further proposes selecting one of the secret keys (K1) stored in the subscriber identification module (SIM) and calculating from the random value RAND and the selected one of the secret keys (K1) a corresponding value for a signed response (SRES) and cipher key (KC) and sending the calculated values by the subscriber identification module (SIM) to the mobile radio network, which compares the signed response (SRES) to all SRES values for the random value RAND and validates the user's authentication if a match is found. See, e.g. p. 4, 1$^{st}$ line-p. 6, 17$^{th}$ line.

Claims 2, 3, 6, and 8 are amended and claims 4, 5, and 7 are canceled to address editorial issues raised by the amendment of independent claim 1, as well as editorial issues in translation of the claims. Support for the foregoing amendment is found throughout the specification and in the claims as detailed above. Accordingly, no new matter has been added.

***Claim Rejections - 35 U.S.C. § 103***

Claims 1-8 stand rejected over Mills (U.S. Patent No. 6,665,529) in view of Tatebayashi (U.S. Patent No. 6,009,174) under 35 U.S.C. 103(a). The rejection is respectfully traversed and reconsideration is requested. The references asserted do not teach or suggest the claimed invention, either separately or in combination with one another.

Regarding independent claim 1, the Examiner considers that Mills teaches each and every claimed element except storing several different secret codes and one code (K1) that is selected for the execution of the authentication, which the Examiner considers to be taught by Tatebayashi. It is true that Mills discloses the conventional authentication procedure that is generally in use in GSM-type digital mobile communication systems, and which is also described in the "Background" section of the present application on page 2, lines 1-12. As pointed out in Mills, and in the "Background" section of the present application, a unique subscriber key (K1) is installed in both the SIM chip in the mobile unit and in the mobile radio network and used by both the SIM and the mobile radio network to generate respective signed responses (SRES) and cipher keys (KC). See, e.g., Mills, Col 5, lines 44-67; Col 6, lines 1-10 and lines 55-64.

However, as acknowledged, by the Examiner, Mills discloses storing a single unique SIM-specific key (KI) rather than several different secret SIM-specific keys (KI) in the mobile radio network and the user's subscriber identification module (SIM), as recited in claim 1. Further, Mills neither teaches nor suggests pre-configuring and storing a RAND/SRES/KC authentication triplet for each one of the several secret keys (K1) stored in the mobile radio network and selecting and sending a random value RAND of one of the pre-configured authentication triplets to the subscriber identification module (SIM) by the mobile radio network, as also recited in claim 1. Neither does Mills teach or suggest selecting one of the several different secret keys (K1) stored in the subscriber identification module (SIM) and calculating from the random value RAND and the

selected one of the secret keys (K1) a corresponding value for a signed response (SRES) and cipher key (KC) and sending the calculated values by the subscriber identification module (SIM) to the mobile radio network, which compares the signed response (SRES) to all SRES values for the random value RAND and validates the user's authentication if a match is found, as likewise recited in claim 1.

Tatebayashi fails to cure the deficiencies of Mills. It is true that Tatebayashi stores multiple secret keys K1, K2 and K3 in a transmission apparatus and a reception apparatus. See, e.g., Tatebayashi , Abstract and Col 3, lines 35-46. However, instead of pre-configuring and storing RAND/SRES/KC authentication triplets for each of the several secret keys, as recited in claim 1, the transmission apparatus of Tatebayashi randomly selects one of the secret keys Ks and (a) generates a carrier message that indicates the secret key Ks, (b) encrypts the carrier message using the secret key Ks, (c) and also encrypts the carrier message using the carrier message itself as the secret key. Further, instead of selecting and sending the random value RAND of one of the pre-configured authentication triplets, as recited in claim 1, Tatebayashi sends both encrypted carrier messages that indicate the secret key Ks to the reception apparatus. See, e.g., Tatebayashi, Abstract and Col 7, lines 33-59.

In addition, instead of selecting one of the secret keys (K1) stored in the subscriber identification module (SIM) and calculating from the received random value RAND and the selected one of the secret keys (K1) a corresponding value for a signed response (SRES) and cipher key (KC), as recited in claim 1, the reception apparatus of Tatebayashi decrypts the carrier message encrypted with the selected key Ks using each one of the stored keys, K1, K2, and K3, and also uses each of those decryptions to decrypt the carrier message that was encrypted with the carrier message itself as the key. See, e.g., Tatebayashi , Abstract and Col 8, lines 4-18.

Moreover, there is not a hint of teaching or suggestion in Tatebayashi of sending the value for a signed response (SRES) and cipher key (KC) calculated from the received random value RAND and the selected one of the secret keys (K1) to the mobile radio network by the subscriber identification module (SIM), as recited in claim 1. Neither is

there any teaching or suggestion whatsoever in Tatebayashi of comparing the signed response (SRES) to all SRES values for the random value RAND by the mobile radio network and validating the user's authentication if a match is found, as likewise recited in claim 1. On the contrary, according to Tatebayashi, the reception apparatus itself simply compares the respective decrypted messages and authorizes the selected key when two of the decrypted messages match one another. See, e.g., Tatebayashi , Abstract and Col 8, line 34-Col 9, line 20.

Consequently, Mills, which teaches the conventional authentication system used in GSM-type digital mobile communications, and Tatebayashi, which teaches a secret key transfer method between a transmission apparatus and a reception apparatus, do not teach or suggest, either separately or in combination with one another, the required combination of limitations of applicants' procedure for the increased security of authentication processes in digital mobile radio systems, as recited in claim 1.

Because the cited references, either alone or in combination, do not teach the limitations of independent claim 1, the Examiner has failed to establish the required *prima facie* case of unpatentability. See In re Royka, 490 F.2d 981, 985 (C.C.P.A., 1974) (holding that a *prima facie* case of obviousness requires the references to teach all of the limitations of the rejected claim); See also MPEP §2143.03. The Examiner has failed to establish the required *prima facie* case of unpatentability for independent claim 1 and similarly has failed to establish a *prima facie* case of unpatentability for claims 2, 3, 6, and 8 that depend on claim 1, and which recite further specific elements that have no reasonable correspondence with the references.

**Conclusion**

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the

application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

Date: 7/14/04

John M. Harrington (Reg. No. 25,592)

Kilpatrick Stockton LLP
1001 West Fourth Street
Winston-Salem, NC 27101
(336) 607-7300